(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 December 2004 (02.12.2004)

PCT

(10) International Publication Number
WO 2004/105307 A1

(51) International Patent Classification⁷: H04L 9/06

(21) International Application Number: PCT/KR2004/001175

(22) International Filing Date: 18 May 2004 (18.05.2004)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2003-0032071 20 May 2003 (20.05.2003) KR

(71) Applicant (*for all designated States except US*): NHN CORPORATION [KR/KR]; 7F., Startower Building, #737, Yeoksam-dong, Gangnam-gu, Seoul 135-080 (KR).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): KANG, Kyungdon [KR/KR]; 190-147 Sadang 5-dong, Dongjak-gu, Seoul 156-095 (KR).

(74) Agent: KIM, Seog-Hyun; 9th Floor, Daekyung Building, 2-ka, Taepyung-ro, Chung-ku, Seoul 100-724 (KR).

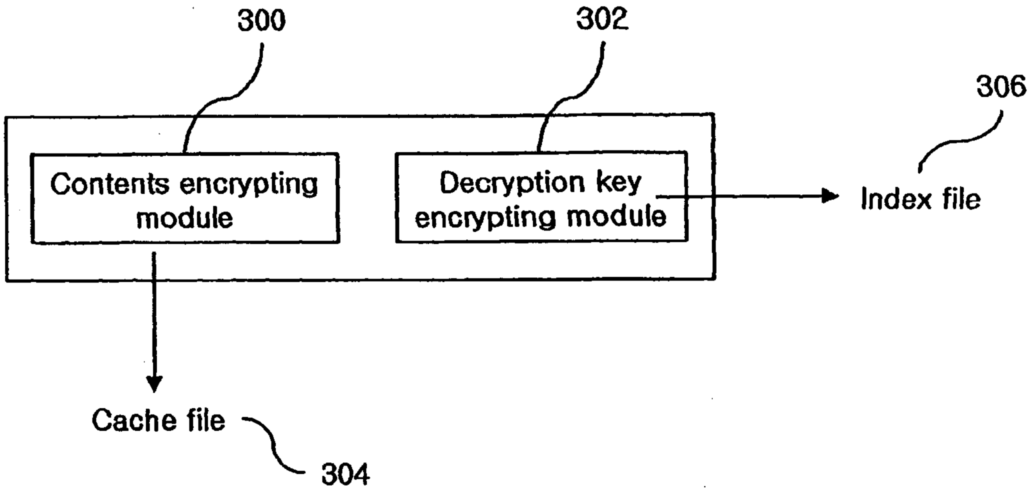
(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND DEVICE OF DATA ENCRYPTION



(57) Abstract: The present invention provides an encryption method and apparatus thereof, by which a user is unable to illegally use contents data stored in his local client and by which contents data stored in a local client can be quickly decrypted so as not to affect playback of contents. The present invention includes a step (a) of receiving the contents data via the network, a step (b) of changing a sequence of the received contents data according to a predetermined algorithm or randomly to store in a form of a cache file, a step (c) of generating a decryption key including information of the changed sequence of the data, and a step (d) of encrypting the decryption key according to a predetermined encryption system, wherein if a playback or transmission of the stored contents is requested, the encrypted decryption key is decrypted and the corresponding data is extracted from the cache file according to the sequence information of the decryption key to be played back or transmitted.

WO 2004/105307 A1

Method and Device of Data Encryption

TECHNICAL FIELD

The present invention relates to a data encryption method and apparatus thereof, and more particularly, to a data encryption method and apparatus thereof, by which data of contents provided to a client is prevented from being illegally used by a user.

BACKGROUND ART

As such an open type network as Internet prevails in use, the security of data spread on networks becomes more important. Internet is advantageous in user's easy accessibility to requested information. Yet, it is highly probable that data may be illegally circulated by an unauthorized distributor.

Hence, many efforts are made to studying and researching a data encryption method enabling only an authorized user to use contents of data. And, various kinds of encryption algorithm have been opened to the public.

Meanwhile, services of providing moving picture contents such movies, animations, and the like via Internet are tending upward. And, such a contents providing service is one-sidedly transmitted from a server to a local client in general.

Hence, the conventional contents security is performed to mainly prevent a user from accessing to a server illegally.

However, as the contents transmission technologies via Internet are more diversified, contents data of a server may be stored in a client. In such a case, a user occasionally enables to use the stored data illegally.

The moving picture data such as movie, animation, or the like has a large volume. Hence, if it takes quite a long time to decrypt the encrypted data, it is unable to play back the data. Hence, an encryption method enabling to perform a quick decryption is needed to avoid affecting the playback of the data as well as to keep the reliance of the encryption.

DISCLOSURE OF THE INVENTION

Accordingly, the present invention is directed to an encryption method and apparatus thereof that substantially obviate one or more of the problems due to limitations and disadvantages of the related art.

An object of the present invention is to provide an encryption method and apparatus thereof, by which a user is unable to illegally use contents data stored in his local client.

Another object of the present invention is to provide an encryption method and apparatus thereof, by which contents data stored in a local client can be quickly decrypted so as not to affect playback of contents.

Additional features and advantages of the invention will be set forth in the description which follows, and in part will be apparent from the description, or may be learned by practice of the invention. The objectives and other advantages of the invention will be realized and attained by the structure particularly pointed out in the written description and claims thereof as well as the appended drawings.

To achieve these and other advantages and in accordance with the purpose of the present invention, as embodied and broadly described, in encrypting contents data received via a network, a contents data encryption method according to the present invention includes a step (a) of receiving the contents data via the network, a step (b) of changing a sequence of the received contents data according to a predetermined algorithm or randomly to store in a form of a cache file, a step (c) of generating a decryption key including information of the changed sequence of the data, and a step (d) of encrypting the decryption key according to a predetermined encryption system, wherein if a playback or transmission of the stored contents is requested, the encrypted decryption key is decrypted and the corresponding data is extracted from the cache file according to the sequence information of the decryption key to be played back or transmitted.

Preferably, the data received in the step (a) is previously dispersed and stored by a predetermined block unit.

More preferably, the data dispersed and stored by the block unit includes a plurality of sub-blocks, each of the sub-blocks includes a plurality of stripes, and in the step (b), a sequence of the stripes included in each of the sub-blocks is changed.

More preferably, the data dispersed and stored by the block unit includes a plurality of sub-blocks and in the step (b), a sequence of the sub-blocks is changed.

More preferably, the data is previously dispersed and stored by the predetermined block unit in a manner including the steps of deciding whether vacant slots exist in the cache file, if the vacant slots exist, selecting one of the vacant slots randomly to store a block in the selected slot, if the vacant slots fail to exist, searching a slot having an oldest access time of block data stored therein, and storing the block data in the searched slot.

Preferably, the step (d) includes the steps of selecting an encryption application point from the decryption key data, generating an encryption key corresponding to the selected application point, and encrypting a corresponding application point using the generated encryption key.

More preferably, the encryption key is a DES key and the encryption of the application point is performed by DES algorithm. More preferably, the encryption key is a Triple-DES key and the encryption of the application point is performed by Triple-DES algorithm.

More preferably, the selected application point is data for the information of the changed sequence among the decryption key data.

To further achieve these and other advantages and in accordance with the purpose of the present invention, in encrypting contents data received via a network, a contents data encryption apparatus includes a contents encrypting means for changing a sequence of the received contents data according to a predetermined algorithm or randomly to store in a form of a cache file and a decryption key encrypting means for encrypting a decryption key for decrypting data encrypted by the contents encrypting means according to a predetermined encryption system, wherein if a playback or transmission of the stored contents is requested, the encrypted decryption key is decrypted and the corresponding data is extracted from the cache file according to the sequence information of the decryption key to be played back or transmitted.

To further achieve these and other advantages and in accordance with the purpose of the present invention, in a data encryption program installed in a client to encrypt contents data received via a network, a program of encrypting data includes a contents encrypting module changing a sequence of the received contents data according to a predetermined algorithm or randomly to store in a form of a cache file and a decryption key encrypting module encrypting a decryption key for decrypting data encrypted by the contents encrypting module according to a predetermined encryption system, wherein if a playback or transmission of the stored contents is requested, the encrypted decryption key is decrypted and the corresponding data is extracted from the cache file according to the sequence information of the decryption key to be played back or transmitted.

To further achieve these and other advantages and in accordance with the purpose of the present invention, in a system including at least one server and a plurality of clients connected to the at least one server via a network, one of the clients receiving node information storing requested contents data from the server to receive the contents data from the server or another client, in encrypting contents data stored in the client, a data encryption method includes a step (a) of storing the contents data received from the server of the another client, a step (b) of changing a sequence of the stored contents data, a step (c) of generating a decryption key including information of the changed sequence of the data, and a step (d) of encrypting the decryption key according to a predetermined encryption system, wherein the sequence-changed contents is stored in a form of a cache file, wherein if a playback or transmission of the sequence-changed contents is requested, the encrypted decryption key is decrypted and the corresponding data is extracted from the cache file according to the sequence information of the decryption key to be played back or transmitted.

It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention and together with the description serve to explain the principles of the invention.

In the drawings:

Fig. 1 is an exemplary diagram of a contents data transmission network where a data encryption method according to the present invention is applied;

Fig. 2 is an exemplary diagram of another transmission system where a data encryption method of the present invention is applied;

Fig. 3 is a block diagram of a module structure of an encryption program according to one preferred embodiment of the present invention;

Fig. 4 is a diagram of showing units of contents data according to one preferred embodiment of the present invention;

Fig. 5 is a block diagram of a contents encrypting module according to one preferred embodiment of the present invention;

Fig. 6 is an exemplary diagram showing that a data sequence change module 502 changes a stripe sequence stripe to vary an attribute of each sub-block;

Fig. 7 is a block diagram of a decryption-key encrypting module according to one preferred embodiment of the present invention;

Fig. 8a is a diagram of a field structure of a decryption key according to one preferred embodiment of the present invention;

Fig. 8b is a diagram of a header field structure of a decryption key according to one preferred embodiment of the present invention;

Fig. 8c is a diagram of a block information field structure of a decryption key according to one preferred embodiment of the present invention;

Fig. 8d is a diagram of a block information field structure of a decryption key according to another embodiment of the present invention;

Fig. 9 is a flowchart of an overall process of an encryption method according to one preferred embodiment of the present invention;

Fig. 10 is an exemplary flowchart of dispersing to store contents data according to one preferred embodiment of the present invention; and

Fig. 11 is a flowchart of a decryption-key encrypting method according to one preferred embodiment of the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

Fig. 1 is an exemplary diagram of a contents data transmission network where a data encryption method according to the present invention is applied.

The present invention relates to encryption to prevent a user from filing contents data stored in user's local client. In this case, the contents data may include moving picture data such as a movie, animation, and the like, still picture data, and document text data such as a novel.

Generally, contents data such as moving picture data is provided to user's local client from a server by real-time streaming. Hence, contents data stored in a server is not stored in user's local client in general.

Yet, as mentioned in the foregoing description, contents transmission technologies in Internet are diversified so that contents data may be stored in user's local client in part or entirely.

Examples of a contents transmission system, in which contents data of a server is stored in a user client, are shown in Fig. 1 and Fig. 2. An encryption method according to the present invention is applicable to such a contents transmission system. The contents transmission systems shown in Fig. 1 and Fig. 2 are just exemplary. In case that contents data is stored in user's local client, an encryption method according to the present invention is applicable to any kind of system as well as to the system shown in Fig. 1 or Fig. 2.

Referring to Fig. 1, a system adopting an encryption method according to the present invention includes a plurality of user clients 102, 104, 106, 108, 110, 112, and 114 connected to a server 100 via a network.

The transmission system, as shown in Fig. 1, is applicable to overlay multicasting. The overlay multicasting is a technology that forwarding of multicast data is performed in an end host or server instead of a router.

When the same data are transferred to a plurality of user clients like Internet broadcasting, multicasting may be effective in use. Yet, in case of transmitting data by multicasting, a previous router should be replaced by a multicast router.

In replacing the previous router by the multicast router, it takes much time as well as high costs. Hence, the overlay multicasting is operative in enabling a user client or server to play a role as the multicast router.

In Fig. 1, it is assumed that the server 100 is transferring Internet broadcast data and the first and second clients 102 and 103 are receiving the data transferred from the server 100.

In case of general unicasting instead of the overlay multicasting, the third client 104 intending to receive the broadcast data transferred from the server 100 directly needs to access the server 100 to receive the broadcast data.

Yet, in case of using the overlay multicasting, the third client 104 accesses the second client 102, thereby enabling to receive the broadcast data the second client 102 receives from the server 100. Namely, the third client 104 receives the broadcast data not from the server 100 in direct but via the second client 102.

In case of adopting the unicasting, the entire clients access the server 100 to request data. Hence, heavy load is put on the server and the server 100 is unable to transfer data to a multitude of the clients.

Yet, in case of adopting the overlay multicasting, the client receives data and simultaneously plays a role as a server transferring the data to other clients. Hence, the server is free from load and the data can be transferred to a multitude of the clients.

In the overlay multicasting, an agent program is installed in each of the clients intending to request data. The agent program enables each of the clients intending to request the data to receive information of other clients receiving the data via the serve 100 and to access the corresponding client to request the data.

By the agent program, the third client 104 recognizes that the second client 102 is receiving the broadcast data via the server 100 and then accesses the second client 102 to request the data.

Such an overlay multicast transmission network is applicable to a VOD (video on demand) system as well as real-time broadcast. The client receives address information of another client storing the corresponding multimedia contents from the server 100 and then receives the corresponding multimedia contents from another client instead of the server. Hence, it is unnecessary for the entire clients to receive the data from the server, whereby the load put on the server can be reduced.

Yet, in case of providing a VOD service via an overlay multicast system, a user client stores contents data in the form of a cache file.

Thus, when the contents data are stored in the client, a user performs filing on the contents data stored in the client and may use it illegally. Hence, a contents encryption method, which is used only in transferring contents data stored in a client to another client and on which a user is unable to perform filing illegally, is requested. An encryption method according to the present invention is applicable to a transmission system of downloading data stored in another user client.

Fig. 2 is an exemplary diagram of another transmission system where a data encryption method of the present invention is applied.

Fig. 2 shows a system as follows. First of all, a server 200 previously transfers contents data to a user client 204. After having stored the transferred contents data, the user client 204 plays back the stored contents data whenever the user wants to. And, such a system provides a service named 'contents reservation function' in general.

Even if data can be provided at relatively high speed since the server 200 secures a relatively wide bandwidth, it may happen that the data is unable to be received at the transfer rate of the server due to a poor network environment between the server and client. For instance, in case that a network link connected to a client supports up to 1Mbps when a server transfers data at 2Mbps, the client is unable to be provided with moving picture data of high resolution provided from the server.

Otherwise, in case of intending to play back contents data, which was previously downloaded while a user was doing something else, the transport system shown in Fig. 2 is applicable thereto.

When the data downloaded via contents reservation is to be played back, the transferred contents should be stored in the user client. Hence, a user may perform filing on the downloaded contents to use illegally as well in case of the contents reservation. Hence, the encryption method according to the present invention is applicable thereto.

Although a basic model of a transmission system enabling contents reservation is illustrated in Fig. 2, it is apparent to those skilled in the art that the contents reservation function is applicable to other contents transmission systems including an overlay multicasting system in Fig. 1 and the like.

Fig. 3 is a block diagram of a module structure of an encryption program according to one preferred embodiment of the present invention.

An encryption method according to the present invention can be implemented via a general computer program. Yet, the encryption method according to the present invention is not limited to the implementation via program. But, it is apparent to those skilled in the art that the encryption method according to the present invention can be implemented in the form of a separate chip, card, or the like.

Referring to Fig. 3, an encryption program according to the present invention may include a contents encrypting module 300 and a decryption-key encrypting module 302.

The contents encrypting module 300 encrypts contents data received from a server or another client.

In case that the contents are multimedia contents, the encrypted data are decrypted to be played back. Hence, if it takes a quite a long time for decryption, contents playback may be affected.

In accordance with one preferred embodiment of the present invention, the contents encrypting module preferably encrypts the contents data in a manner that no time delay for decrypting the contents data almost occurs.

General encryption algorithm according to a related art needs quite a longer time delay in decryption, thereby being hardly applicable to the present invention.

Hence, the contents encrypting module according to the preferred embodiment of the present invention preferably performs encryption in a manner of changing a sequence of contents data. In case of changing sequence of the contents data, it is able to perform decryption without a time delay since the decryption is enabled by recognizing the changed sequence information only without decrypting the encrypted data via a specific decryption function.

The contents data of which sequence is changed by the contents encrypting module is stored in a cache file 304.

Moreover, the contents encrypting module generates a decryption key including information of the changed sequence.

Meanwhile, the decryption-key encrypting module 302 is operative in encrypting again the decryption key of the data encrypted by the contents encrypting module 300 according to a predetermined encryption algorithm. The contents encrypting module performs encryption in a manner of changing the sequence information of the data only, whereby its reliance of security may not be better than that of other encryption algorithm. Yet, a decryption time should avoid affecting the playback of the contents data, whereby it is unable to use a encryption algorithm having higher reliance of security in encrypting the contents data.

Accordingly, the decryption-key encrypting module 302 encrypts decryption-key data, of which decryption time is short due to small capacity, again. The decryption-key encrypting module 302 can encrypt the decryption key using a general encryption algorithm.

The decryption-key encrypting module 302 according to the present invention may encrypt the decryption key using a symmetric-key encrypting system.

The symmetric-key encrypting system is a system that a sender or recipient performs encryption and decryption processes using the same key. As a symmetric-key encrypting system, there are American DES (data encryption standard), Triple-DES, European IDEA (international data encryption algorithm), Japanese FEAL (fast data encryption algorithm), etc.

In accordance with another embodiment of the present invention, a public-key encrypting system is also applicable to the encryption of the decryption key.

The public-key encrypting system differs in encryption and decryption keys. Even if one of the encryption and decryption keys in the public-key encrypting system is known, it is difficult to know the other. In the public-key encrypting system, a pair of keys are generated via a key generation algorithm, one is opened to the public, and the other is kept as a secret key to use.

As a public-key encrypting system, there are RSA encryption using difficulty of factorization, Rabin encryption, Merkle-Hellman Knapsack encryption, Graham-Shamor encryption, MeEliece encryption using difficulty in decrypting a linear error correction sign, elliptic curve encryption system, etc.

The decryption key encrypted by the decryption-key encrypting module 302 is stored in the form of index file 306.

Fig. 4 is a diagram of showing units of contents data according to one preferred embodiment of the present invention.

Referring to Fig. 4, contents data in an encryption method according to the present invention can be divided into a resource 400, a block 402, a sub-block 404, and a stripe 406, in turn.

Each of the resource 400, block 402, sub-block 404, and stripe 406 in Fig. 4 is a name for unit of storing or encrypting data for convenience of distinction. And, it is apparent to those skilled in the art that units of the contents data can be divided in a manner different from that shown in Fig. 4.

The resource 400 in Fig. 4 is overall data for one contents. The resource 400, as shown in Fig. 4, includes a plurality of blocks 402. In accordance with one embodiment of the present invention, the block may consist of 16 Mbytes.

The block 402 includes a plurality of sub-blocks 404. In accordance with one preferred embodiment of the present invention, the sub-block may consist of 1 Mbytes, In this case, the block 402 includes sixteen sub-blocks 404.

The sub-block 404 includes a plurality of stripes 406. In accordance with one preferred embodiment of the present invention, the stripe may consist of 32 Kbytes. In this case, the sub-block 404 includes thirty-two stripes.

Fig. 5 is a block diagram of a contents encrypting module according to one preferred embodiment of the present invention.

Referring to Fig. 5, a contents encrypting module according to one preferred embodiment of the present invention includes a storage location control module 500, a data sequence change module 502, and a decryption-key generating module 504.

The storage location control module 500 is to control a location where contents data is stored. In accordance with one embodiment of the present invention, the contents data is stored in a cache file by block unit. In doing so, the storage location control module 500 controls a storage location of block data so that the contents data is stored in a random location instead of a sequential location.

Namely, the contents encrypting module primarily disperses to store the contents data by the block unit by the storage location control module 500, thereby preventing a user from performing filing on the contents data. A detailed method of dispersing the storage location of block will be explained by referring to the attached drawings later.

The data sequence change module 502 changes a sequence of stripes included in a sub-block. For instance, in case that 1st to 32nd stripes are sequentially included in a sub-block while not being encrypted, the data sequence change module 502 randomly changes a sequence of the sequentially arranged stripes.

Fig. 6 is an exemplary diagram showing that a data sequence change module 502 changes a stripe sequence to vary an attribute of each sub-block.

Referring to Fig. 6, a block 600 includes a plurality of sub-blocks 602, and a plurality of stripes are sequentially arranged in each of the sub-blocks 602. The data sequence change module changes a sequence of the stripes, by which an attribute of a block 1 is transformed into a block 1'.

Encryption can be achieved in a manner of changing a sequence of the sub-blocks instead of changing the sequence of the stripes included in each of the sub-blocks in Fig. 6.

The decryption-key generating module 504 records the changed sequence information in a decryption key so that the sequence information changed by the data sequence change module 502 can be decrypted later.

And, the decryption-key generating module 504 enables to record location information of the dispersed and stored block. If the sequence of the data stored in the cache file is equal to that of the data recorded in the decryption key, it will be unnecessary for the decryption-key generating module to record the information of the storage location in a separate field.

Fig. 7 is a block diagram of a decryption-key encrypting module according to one preferred embodiment of the present invention.

Referring to Fig. 7, a decryption-key encrypting module according to one preferred embodiment of the present invention includes an application point selecting module 700, a DES key selecting module 702, and an application point encrypting module 704.

Fig. 7 shows a module in case of encrypting a decryption key using the DES or Triple-DES system. As mentioned in the foregoing description, various encryption algorithms can be used in the decryption-key encryption.

The application point selecting module 700 selects application points for performing DES encryption thereon. In accordance with the preferred embodiment of the present invention, encryption is preferably performed on partially selected application points instead of the entire decryption key to minimize a time taken for decryption. And, the application point selecting module 700 selects partial application points on which the encryption will be performed among the entire decryption key data. For instance, if the decryption key includes total M bytes, there are M selectable application points and the application point selecting module selects N of M.

The application point selecting module 700 enables to randomly select application points, on which decryption will be performed, from the entire decryption key data. In accordance with another embodiment of the present invention, the application point selecting module 700 may previously select application points by a predetermined selection algorithm.

In case of selecting application points randomly, the selected application point information needs to be managed as separate index information. In case of selecting application points by the predetermined selection algorithm, the selected application point information needs not to be managed as separate index information only if the number of application points is known.

Data for data sequence change information is the most important one among the entire decryption key data, whereby the selected application points are preferably data for the sequence change information among the decryption key data.

The DES key selecting module 702 selects a DES key for the respective selected application points. In accordance with one embodiment of the present invention, the DES key for the respective application points can be randomly selected. In accordance with another embodiment of the present invention, DES-key selection algorithm for each application point may be previously configured.

In case of selecting the DES key randomly, application points and DES key information corresponding to the application points need to be managed as a separate index file. Yet, in case of selecting the DES key for the application point via the previously configured selection algorithm, the DES key information corresponding to the application point needs not to be managed as an index file.

The application point encrypting module 704 performs encryption on the selected application point with the corresponding DES key. If N application points are selected, encryption is performed total N-times. The DES encryption system is already opened to the public and its detailed explanation will be skipped in the following description.

Fig. 8a is a diagram of a field structure of a decryption key according to one preferred embodiment of the present invention.

Referring to Fig. 8a, a decryption key according to one embodiment of the present invention includes a header field 800 and a plurality of block information fields 802. As contents data are stored in a cache file by block unit, so does information in the decryption key by block unit.

Fig. 8b is a diagram of a header field structure of a decryption key according to one preferred embodiment of the present invention.

Referring to Fig. 8b, a header includes a file Id field 804 and a version field 806.

In case that there are a plurality of decryption key files, the file ID field need information to identify the decryption file keys. And, version information of the decryption key is recorded in the version field 806.

Fig. 8c is a diagram of a block information field structure of a decryption key according to one preferred embodiment of the present invention.

Referring to Fig. 8c, a block information field structure of a decryption key according to one preferred embodiment of the present invention includes a resource

ID information 810, a block number information 812, a sub-block mask information 814, a stripe number information 816, a checksum information 818, and an access time information 820.

The resource ID information 810 means a unique ID of a resource (contents) including a block therein. For instance, if the contents is the movie 'gone with the wind', the unique ID information indicating the corresponding movie will be recorded as the resource ID information.

Number information of each block is recorded in the block number 812, and information of whether a sub-block includes stripes therein is recorded in the sub-block mask 814. For instance, if there exists no stripe, '0' is recorded. If there exist stripes, '1' is recorded.

The checksum information 818 is the data to decide whether stripe data is valid or not. And, time information of final access to the corresponding block lately is recorded in the access time 820.

Fig. 8d is a diagram of a block information field structure of a decryption key according to another embodiment of the present invention, in which a block of cache file and a block of decryption key are recorded in the same sequence. As the block of cache file and the block of decryption key are recorded in the same sequence, information of storage location of the block is not included in the block information.

Yet, information of a storage location 824, as shown in Fig. 8d, can be included in block information.

Fig. 9 is a flowchart of an overall process of an encryption method according to one preferred embodiment of the present invention.

Referring to Fig. 9, a client receives contents data from a server (S900). In accordance with one embodiment of the present invention, the client enables to receive the data by stripe unit.

Instead of storing the received data sequentially, the client disperse the data to store in a cache file (S902). As mentioned in the foregoing description, the client can disperse to store the data by the block unit or by another data unit.

The dispersed and stored data is encrypted in a manner of changing its sequence (S904). As mentioned in the foregoing description, encryption can be performed in a manner of changing the sequence of the stripes included in the sub-block or the sequence of the sub-blocks themselves.

While the encryption progresses in a manner of changing the sequence of data, a decryption key including the changed sequence information is generated to decrypt the encrypted data (S906).

After completion of the sequence-changing encryption, an encrypting process for the decryption key is carried out (S908).

As mentioned in the foregoing description, various encryption algorithms can be utilized for the encryption of the decryption key.

Fig. 10 is an exemplary flowchart of dispersing to store contents data according to one preferred embodiment of the present invention.

Referring to Fig. 10, it is preferentially decided whether vacant slots to store a block therein exist in a cache file (S1000).

If the vacant slots exist in the cache file, one of them is randomly selected and the corresponding block is stored in the selected slot (S1004).

If the vacant slots fail to exist in the cache file, it is decided whether slots for an unreserved resource exist (S1002). In this case, the reserved resource means a resource failing to be played back yet despite previously being downloaded by a user's request of reservation.

If the slots for the unreserved resource exist, one of the existing slots is selected (S1008). In accordance with one embodiment of the present invention, the slot having the oldest access time of the block is selected from the slots storing unreserved blocks. In accordance with another embodiment of the present invention, one of the existing slots can be randomly selected.

Once the corresponding slot is selected in the step S1008 or S1004, the corresponding block is stored in the selected slot (S1010).

The contents dispersing/storing process in case of supporting a reservation function is explained in Fig. 10. Yet, in case of failing to support the reservation function, the step (S1002) of deciding the presence or non-presence of the slot for the unreserved resource can be omitted.

Moreover, it is also able not to select the slot for a reserved resource by setting an access time of the reserved resource to a latest time.

Fig. 11 is a flowchart of a decryption key encrypting method according to one preferred embodiment of the present invention.

Fig. 11 shows a decryption-key encrypting process in case of using Triple-DES system for decryption-key encryption. As mentioned in the foregoing description, in the decryption-key encryption, various encryption algorithms can be used for the decryption-key encryption as well as Triple-DES.

Referring to Fig. 11, an application point for applying DES encryption thereto is selected (S1100). In accordance with one embodiment of the present invention, a DES application point is selected according to a predetermined pattern. In accordance with another embodiment of the present invention, a DES application point can be randomly selected as well. In case of selecting the DES application point randomly, application point selection information should be stored in a separate index file. Hence, the DES application point is more preferably selected according to the predetermined pattern. As mentioned in the foregoing description, the selected DES application point is preferably data for the sequence information among the decryption key data.

After completion of selecting the application point, a DES key for encrypting each application point according to a predetermined algorithm is selected (S1102). In Triple-DES, three encryption keys are used. In this case, the three keys are preferably selected to be uniform. In accordance with one embodiment of the present invention, a remainder found by dividing $n^2/13$ by 4 can be used as a DES key selecting equation, where n is a number of application point.

Once the DES key corresponding to each application point is selected, the application points are encrypted by the corresponding DES keys, respectively (S1104).

INDUSTRIAL APPLICABILITY

Accordingly, the present invention provides the data encryption method and apparatus thereof, by which the contents data stored in the user's local client can be effectively prevented from being illegally used by the user.

Moreover, the encryption method according to the present invention enables to perform the decryption in a short time, thereby having no influence on playback of the data even if the data are encrypted.

While the present invention has been described and illustrated herein with reference to the preferred embodiments thereof, it will be apparent to those skilled in the art that various modifications and variations can be made therein without departing from the spirit and scope of the invention. Thus, it is intended that the present invention covers the modifications and variations of this invention that come within the scope of the appended claims and their equivalents.

WHAT IS CLAIMED IS:

1. In encrypting contents data received via a network, a contents data encryption method comprising:

a step (a) of receiving the contents data via the network;

a step (b) of changing a sequence of the received contents data according to a predetermined algorithm or randomly to store in a form of a cache file;

a step (c) of generating a decryption key including information of the changed sequence of the data; and

a step (d) of encrypting the decryption key according to a predetermined encryption system,

wherein if a playback or transmission of the stored contents is requested, the encrypted decryption key is decrypted and the corresponding data is extracted from the cache file according to the sequence information of the decryption key to be played back or transmitted.

2. The method of claim 1, wherein the data received in the step (a) is previously dispersed and stored by a predetermined block unit.

3. The method of claim 2, wherein the data dispersed and stored by the block unit comprises a plurality of sub-blocks, wherein each of the sub-blocks comprises a plurality of stripes, and wherein in the step (b), a sequence of the stripes included in each of the sub-blocks is changed.

4. The method of claim 2, wherein the data dispersed and stored by the block unit comprises a plurality of sub-blocks and wherein in the step (b), a sequence of the sub-blocks is changed.

5. The method of claim 2, wherein in the step (d), the decryption key is encrypted using one encryption system selected from the group consisting of a symmetric key encryption system and a public key encryption system.

6. The method of claim 2, wherein the data is previously dispersed and stored by the predetermined block unit in a manner comprising the steps of:

deciding whether vacant slots exist in the cache file;

if the vacant slots exist, selecting one of the vacant slots randomly to store a block in the selected slot;

if the vacant slots fail to exist, searching a slot having an oldest access time of block data stored therein; and

storing the block data in the searched slot.

7. The method of claim 1, the step (d) comprising the steps of:

selecting an encryption application point from the decryption key data;

generating an encryption key corresponding to the selected application point; and

encrypting a corresponding application point using the generated encryption key.

8. The method of claim 7, wherein the application point is randomly selected for a portion of the decryption key data.

9. The method of claim 7, wherein the application point is randomly selected according to a predetermined algorithm for a portion of the decryption key data.

10. The method of claim 7, wherein the encryption key corresponding to the application point is randomly generated.

11. The method of claim 7, wherein the encryption key corresponding to the application point is generated according to a predetermined selection algorithm to correspond to an application point number.

12. The method of claim 7, wherein the encryption key is a DES key and wherein the encryption of the application point is performed by DES algorithm.

13. The method of claim 7, wherein the encryption key is a Triple-DES key and wherein the encryption of the application point is performed by Triple-DES algorithm.

14. The method of claim 7, wherein the selected application point is data for the information of the changed sequence among the decryption key data.

15. In encrypting contents data received via a network, a contents data encryption apparatus comprising:

a contents encrypting means for changing a sequence of the received contents data according to a predetermined algorithm or randomly to store in a form of a cache file; and

a decryption key encrypting means for encrypting a decryption key for decrypting data encrypted by the contents encrypting means according to a predetermined encryption system,

wherein if a playback or transmission of the stored contents is requested, the encrypted decryption key is decrypted and the corresponding data is extracted from the cache file according to the sequence information of the decryption key to be played back or transmitted.

16. The apparatus of claim 15, the contents encrypting means comprising:

a storage location control means for dispersing to store the contents data by a predetermined block unit;

a data sequence change means for changing a sequence of the dispersed and stored block data; and

a decryption key generating means for generating the decryption key for decrypting the sequence-changed data.

17. The apparatus of claim 16, wherein the block comprises a plurality of sub-blocks, wherein each of the sub-blocks comprises a plurality of stripes, and

wherein the data sequence change means changes a sequence of the stripes.

18. The apparatus of claim 16, wherein the block comprises a plurality of sub-blocks and wherein the data sequence change means changes a sequence of the sub-blocks.

19. The apparatus of claim 15, the decryption key encrypting means comprising:

an application point selecting means for selecting an encryption application point from the decryption key data;

an encryption key generating means for generating an encryption key corresponding to the selected application point; and

an application point encrypting means for encrypting a corresponding application point using the generated encryption key.

20. The method of claim 19, wherein the application point is data for changed sequence information of decryption key data.

21. In a data encryption program installed in a client to encrypt contents data received via a network, a program of encrypting data, comprising:

a contents encrypting module changing a sequence of the received contents data according to a predetermined algorithm or randomly to store in a form of a cache file; and

a decryption key encrypting module encrypting a decryption key for decrypting data encrypted by the contents encrypting module according to a predetermined encryption system,

wherein if a playback or transmission of the stored contents is requested, the encrypted decryption key is decrypted and the corresponding data is extracted from the cache file according to the sequence information of the decryption key to be played back or transmitted.

22. The program of claim 21, wherein the block comprises a plurality of sub-blocks, wherein each of the sub-blocks comprises a plurality of stripes, and wherein the contents encrypting module changes sequence information of the stripes.

23. The program of claim 21, wherein the block comprises a plurality of sub-blocks and wherein the contents encrypting module changes sequence information of the sub-blocks.

24. In a system including at least one server and a plurality of clients connected to the at least one server via a network, one of the clients receiving node information storing requested contents data from the server to receive the contents data from the server or another client, in encrypting contents data stored in the client, a data encryption method comprising:

a step (a) of storing the contents data received from the server of the another client;

a step (b) of changing a sequence of the stored contents data;

a step (c) of generating a decryption key including information of the changed sequence of the data; and

a step (d) of encrypting the decryption key according to a predetermined encryption system,

wherein the sequence-changed contents is stored in a form of a cache file, wherein if a playback or transmission of the sequence-changed contents is requested, the encrypted decryption key is decrypted and the corresponding data is extracted from the cache file according to the sequence information of the decryption key to be played back or transmitted.

25. The method of claim 24, wherein the data received in the step (a) is previously dispersed and stored by a predetermined block unit.

26. The method of claim 25, wherein the data dispersed and stored by the block unit comprises a plurality of sub-blocks, wherein each of the sub-blocks comprises a plurality of stripes, and wherein in the step (b), a sequence of the stripes included in each of the sub-blocks is changed.

27. The method of claim 25, wherein the data dispersed and stored by the block unit comprises a plurality of sub-blocks and wherein in the step (b), a sequence of the sub-blocks is changed.

Fig. 1

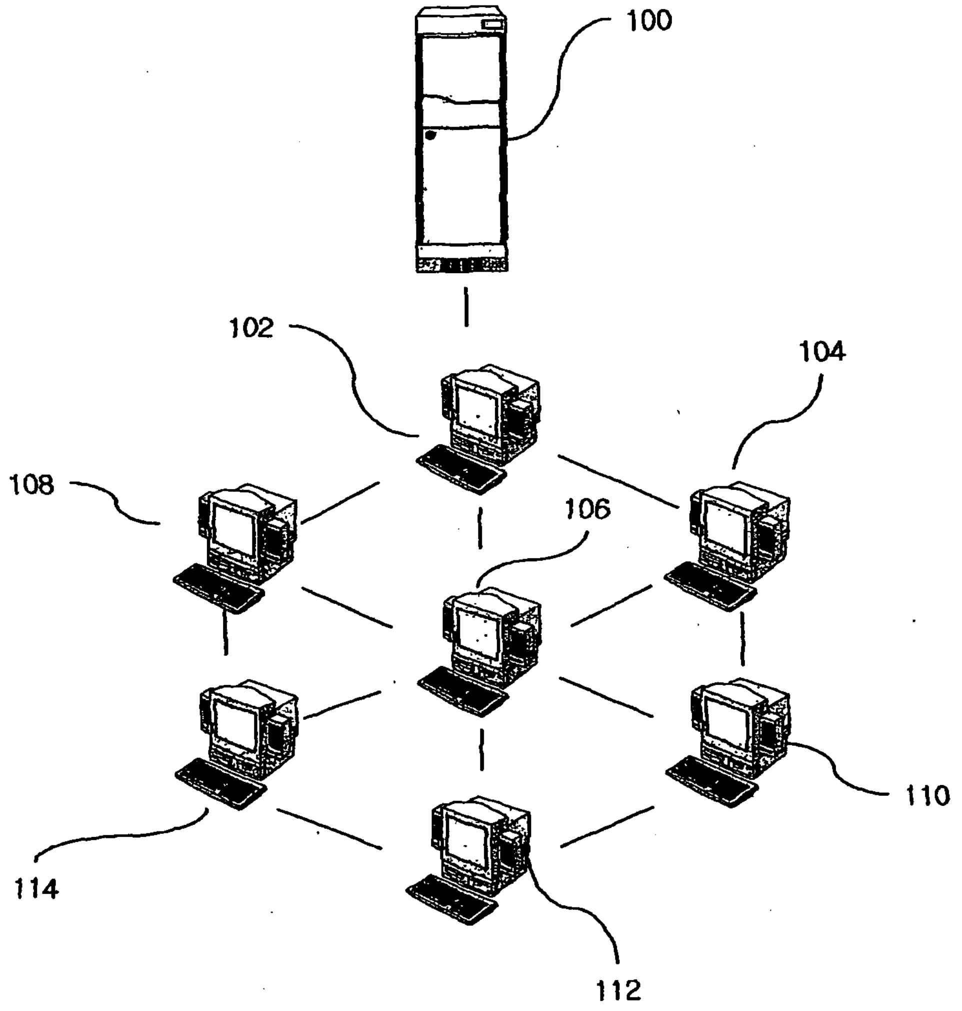


Fig. 2

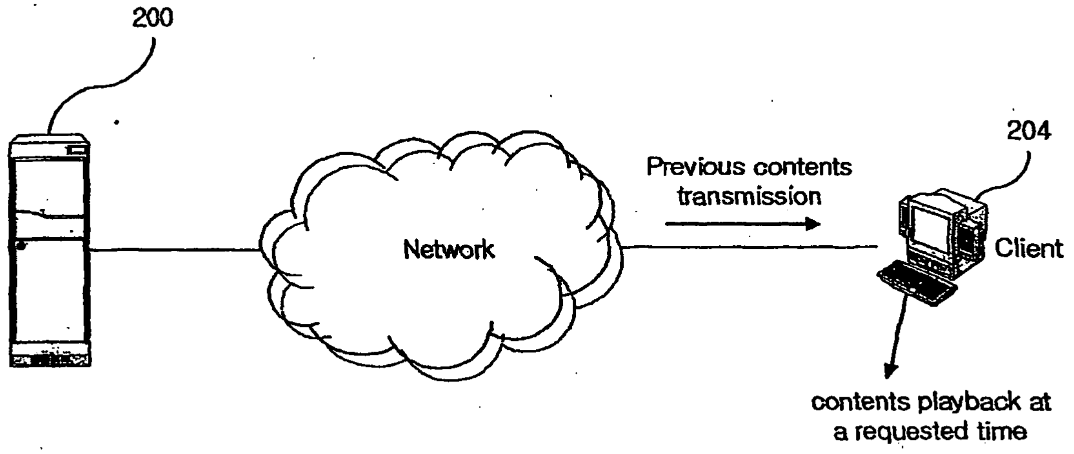

200
Network
Previous contents transmission
204
Client
contents playback at a requested time

Fig. 3

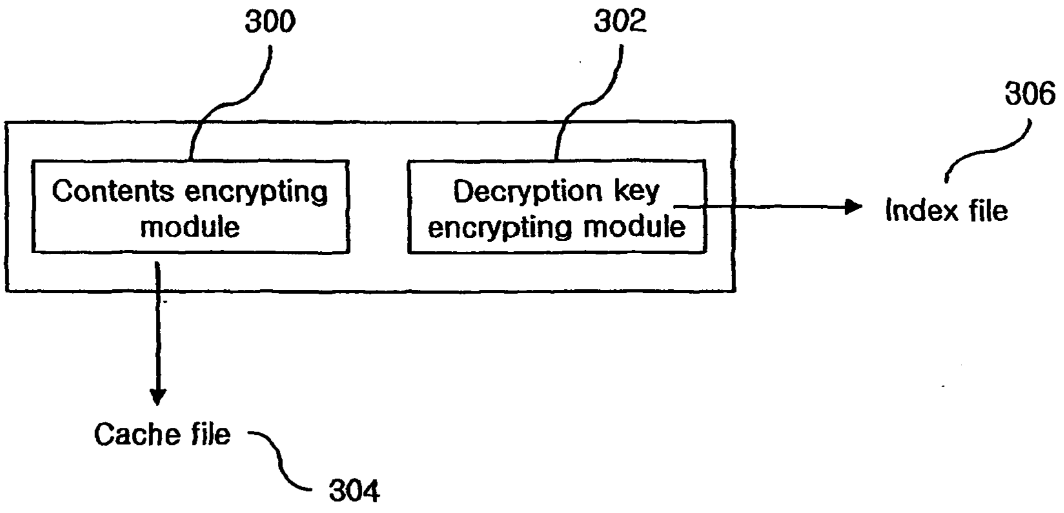

300
302
306
Contents encrypting module
Decryption key encrypting module
Index file
Cache file
304

Fig. 4

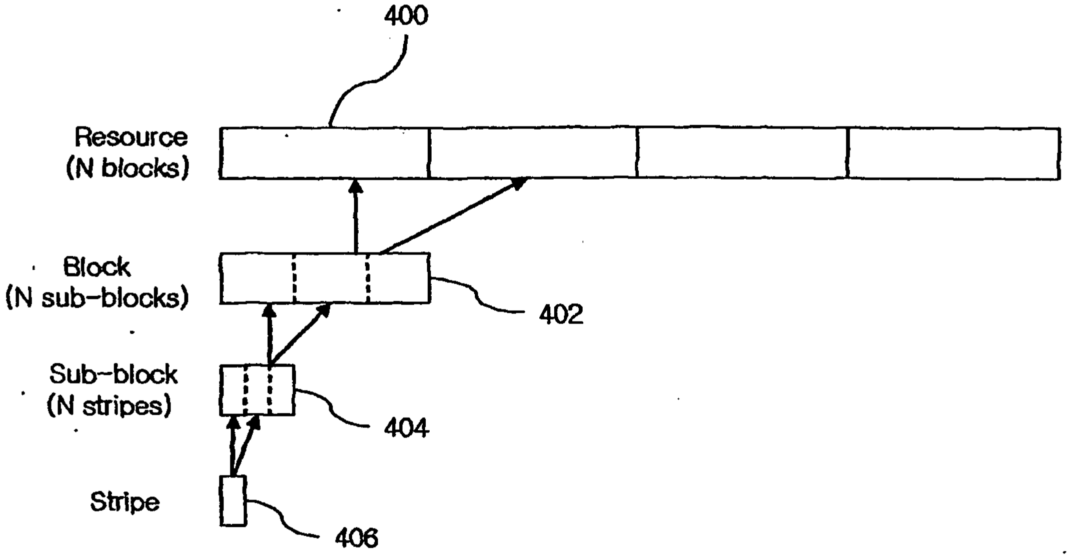

400
Resource
(N blocks)
Block
(N sub-blocks)
402
Sub-block
(N stripes)
404
Stripe
406

Fig. 5

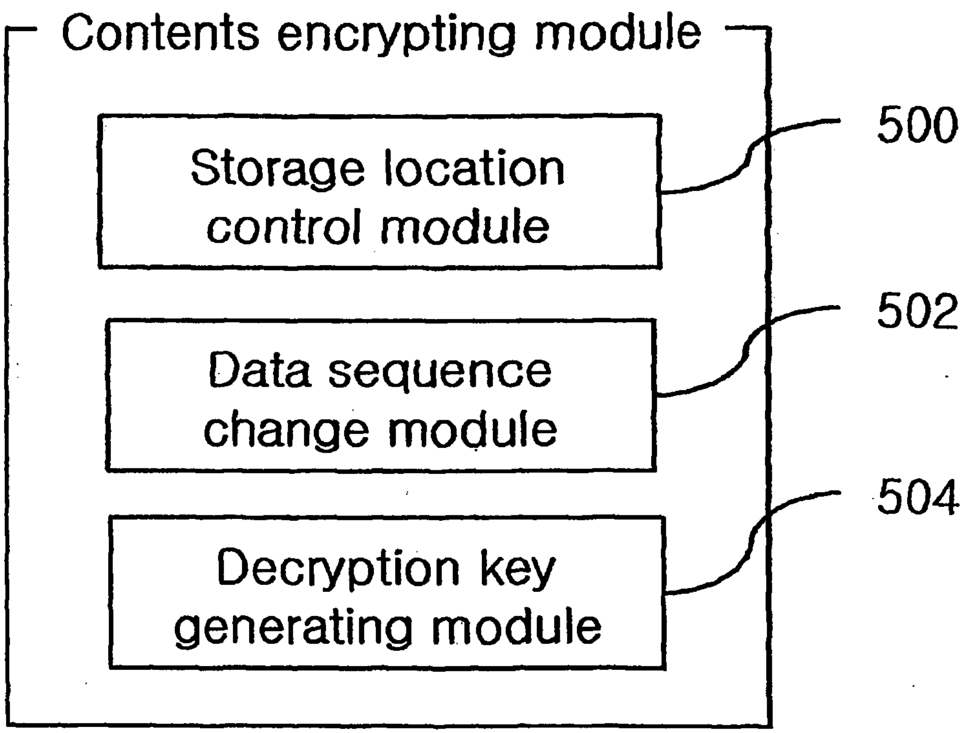

Contents encrypting module
Storage location control module
500
Data sequence change module
502
Decryption key generating module
504

Fig. 6

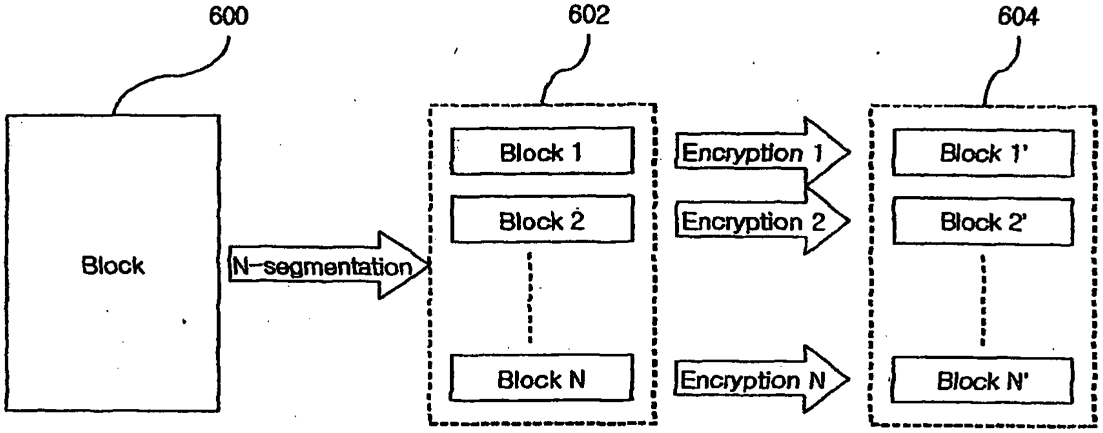

600
602
604
Block
N-segmentation
Block 1
Block 2
Block N
Encryption 1
Encryption 2
Encryption N
Block 1'
Block 2'
Block N'

Fig. 7

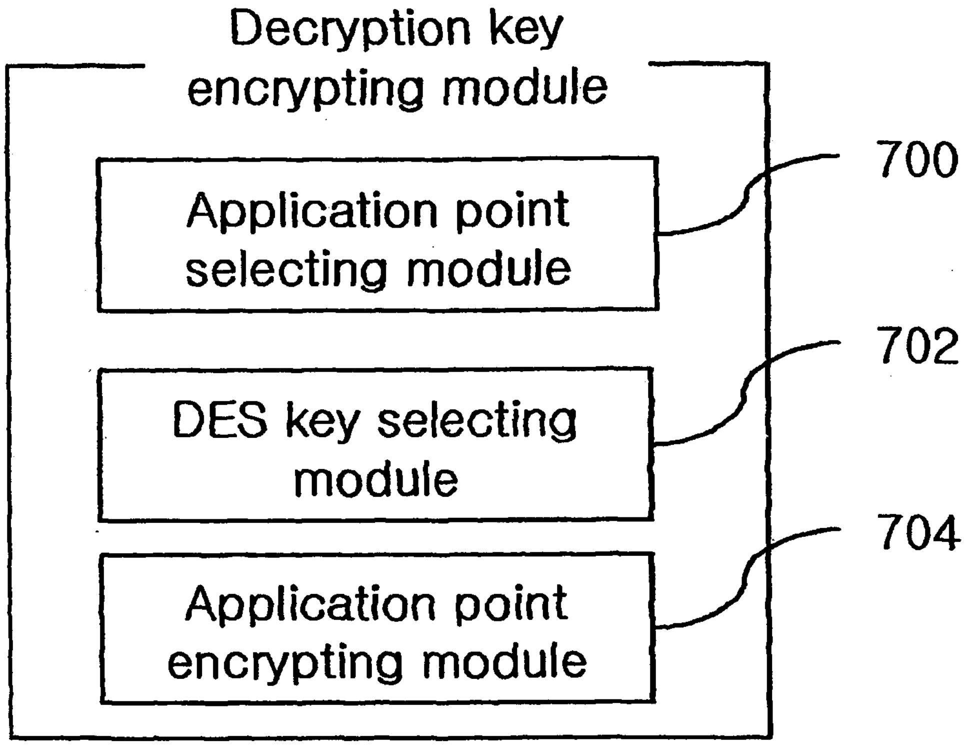

Decryption key encrypting module
Application point selecting module
700
DES key selecting module
702
Application point encrypting module
704

Fig. 8a

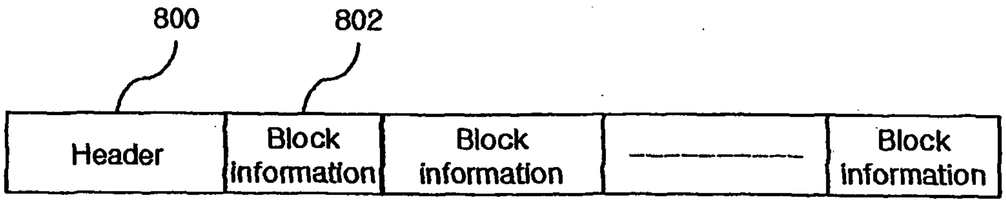


Fig. 8b

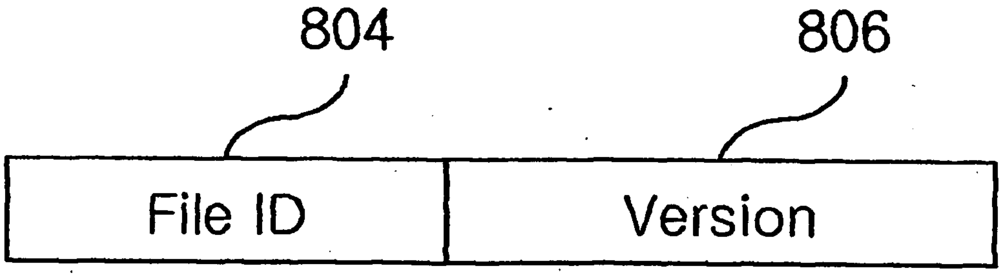


Fig. 8c

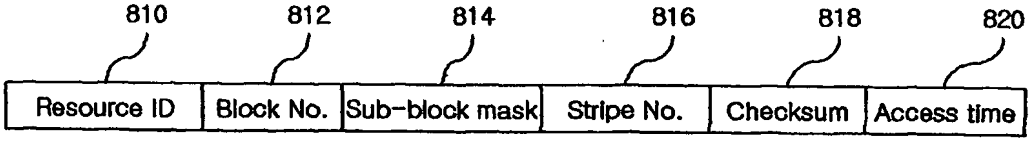


Fig. 8d

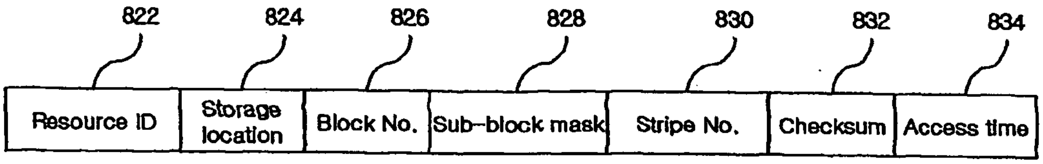


Fig. 9

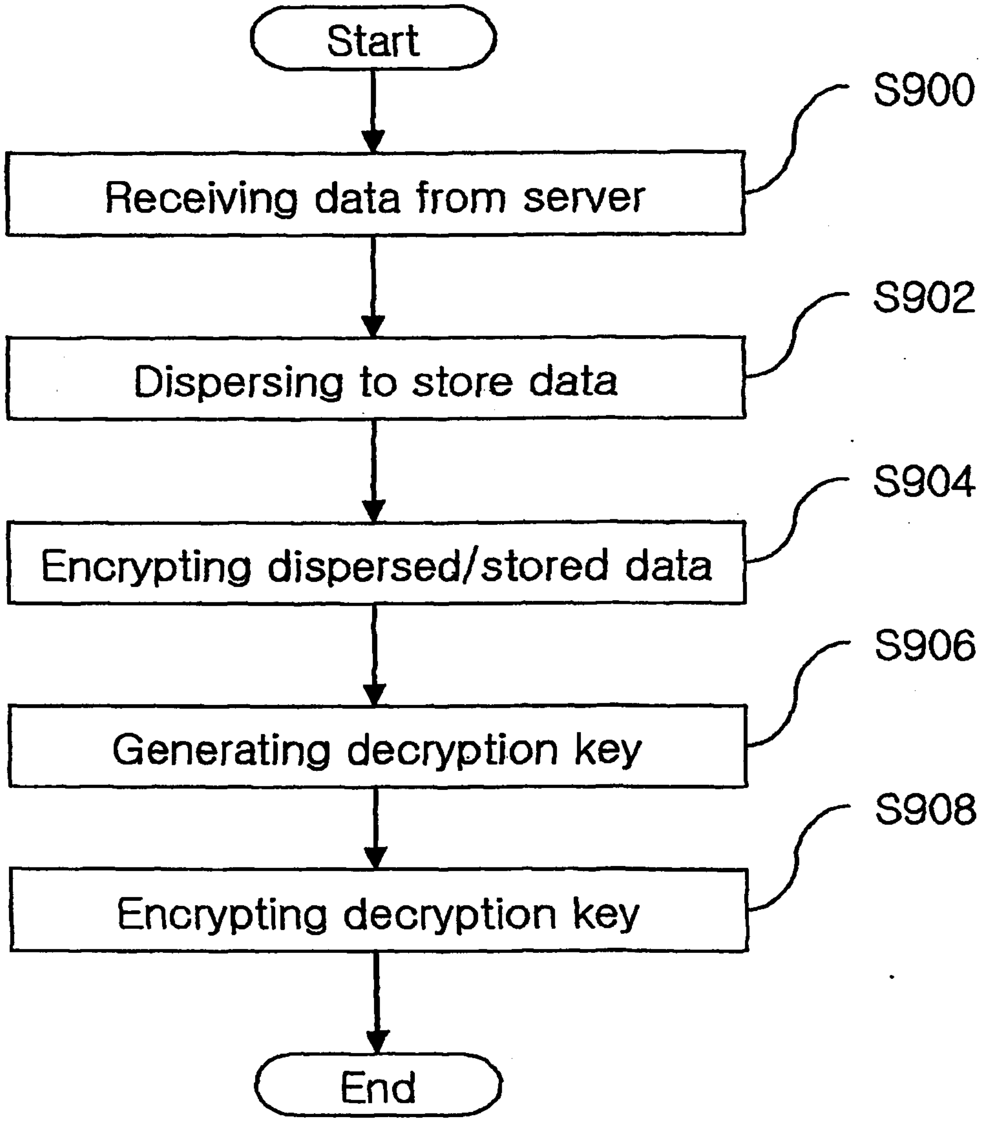

Start
S900
Receiving data from server
S902
Dispersing to store data
S904
Encrypting dispersed/stored data
S906
Generating decryption key
S908
Encrypting decryption key
End

Fig. 10

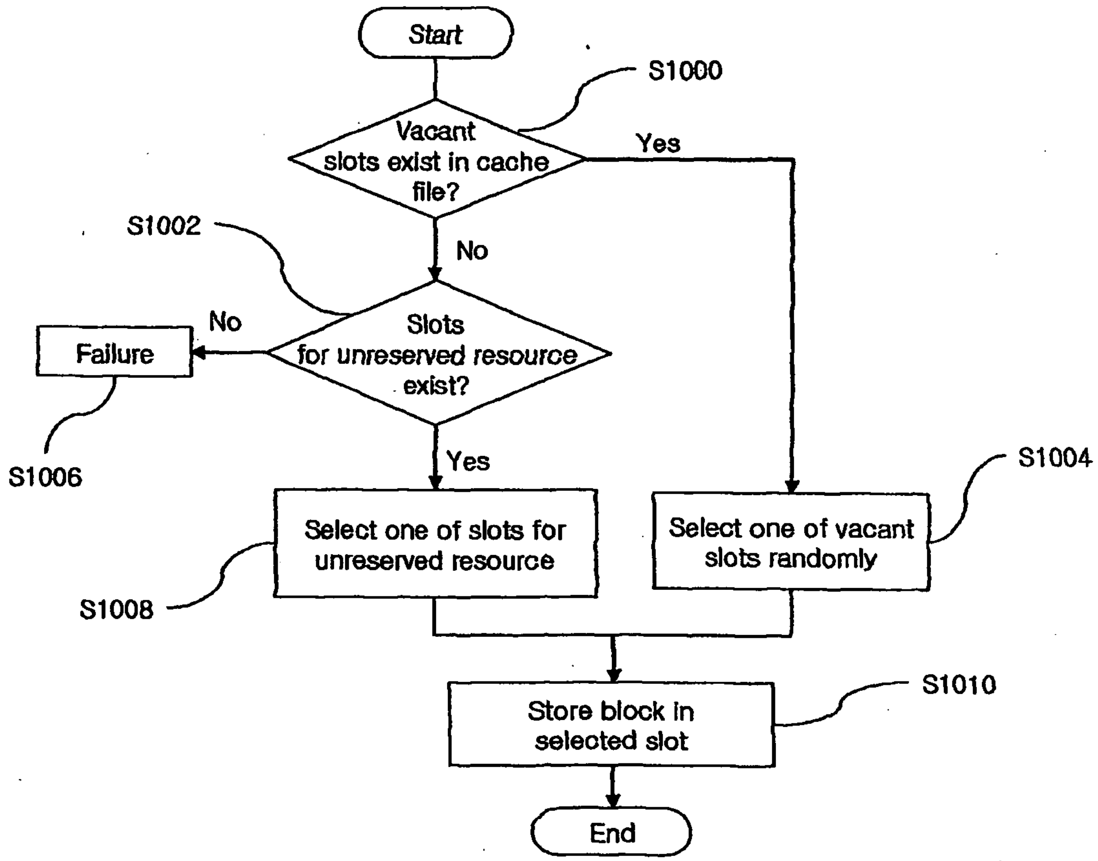
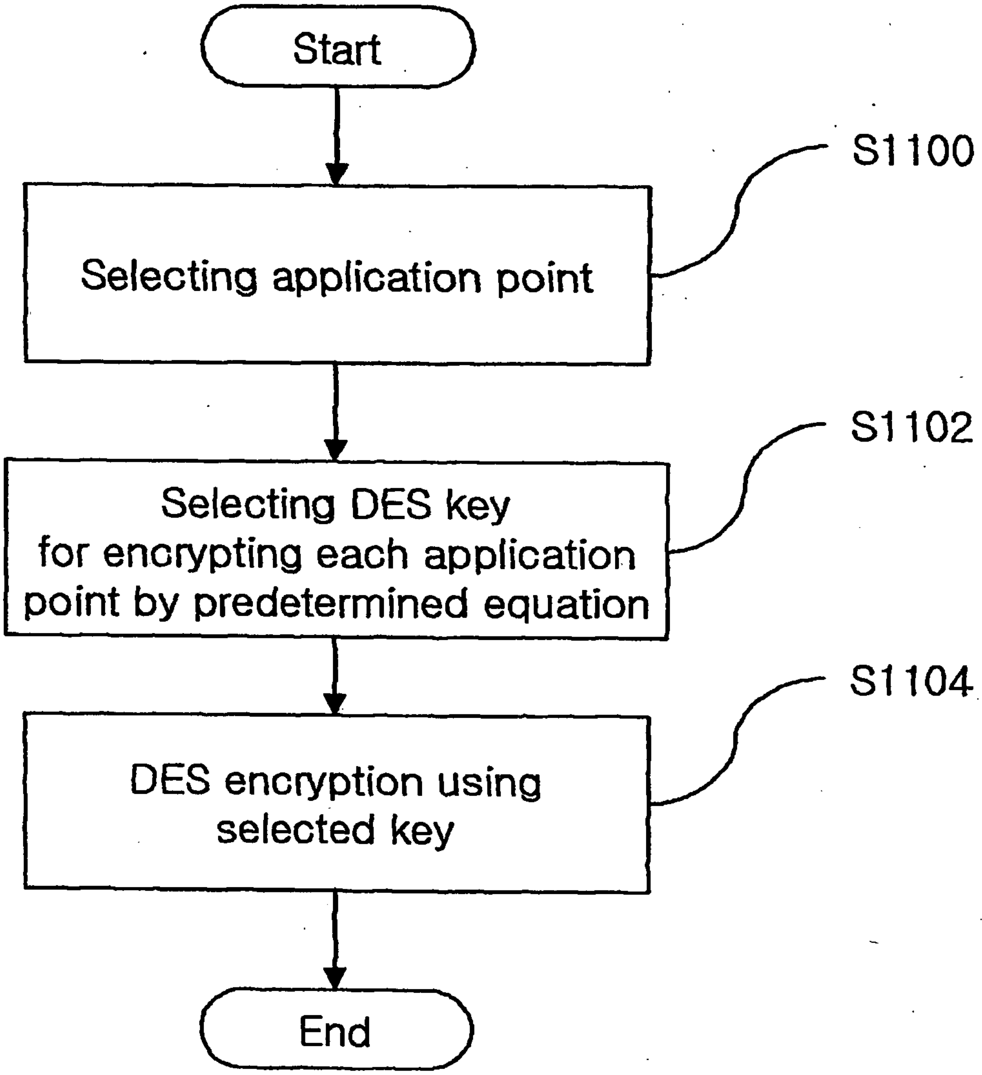

Start
S1000
Vacant slots exist in cache file?
Yes
No
S1002
Slots for unreserved resource exist?
No
Failure
S1006
Yes
S1004
Select one of slots for unreserved resource
Select one of vacant slots randomly
S1008
Store block in selected slot
S1010
End

Fig. 11


Start
S1100
Selecting application point
S1102
Selecting DES key for encrypting each application point by predetermined equation
S1104
DES encryption using selected key
End

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2004/001175

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L 9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/00, 18, 28, 32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search terms used)

search terms : encryption, sequence, order, block, encryption key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1122099 A3 12 Sep. 2001 (Hitachi Ltd.) claims 1, 9	1, 2, 4, 15, 16, 18, 21-25, 27
Y	US 5838795 A 17 Nov. 1998 (Teledyne Industries Inc.) claim 1	1, 2, 4, 15, 16, 18, 21-25, 27
Y	US 5799089 A 25 Aug. 1998 (Irdeto B. V.) claims 1, 10, 11	1, 2, 4, 15, 16, 18, 21-25, 27
A	JP 2002-341759 A 29 Nov. 2002 (Victor Co. of Japan) see summary of the invention	1, 2, 4, 15, 16, 18, 21-25, 27
A	WO 0239654 A1 16 May 2002 (Kozuka Seiichiro) see summary of the invention	1, 2, 4, 15, 16, 18, 21-25, 27
A	US 6055316 A 25 Apr. 2000 (Sun Microsystems Inc.) claims 1, 11, 30, 40	1, 2, 4, 15, 16, 18, 21-25, 27

□ Further documents are listed in the continuation of Box C.   ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 AUGUST 2004 (30.08.2004)	30 AUGUST 2004 (30.08.2004)

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea	JEONG, Jae Woo
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-5718

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2004/001175

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1122099 A3	12 Sep. 2001	US 20010021253 A1 JP 2001-324925 A	13 Sep. 2001 22 Nov. 2001
US 5838795 A	17 Nov. 1998	WO 97/025799 A1	17 July 1997
US 5799089 A	25 Aug. 1998	WO 95/010906 A1 EP 0723726 A1	20 Apr. 1995 31 July 1996
JP 2002-341759 A	29 Nov. 2002	US 20020131596	19 Sep. 2002
WO 0239654 A1	16 May 2002	None	
US 6055316 A	25 Apr. 2000	WO 99/034548 A3 EP 1066700 A2	8 July 1999 10 Jan. 2001